(12) UK Patent Application (19) GB (11) 2 374 718 (13) A

(43) Date of A Publication 23.10.2002

(21) Application No 0109034.9

(22) Date of Filing 11.04.2001

(51) INT CL[7]
G11B 20/00

(52) UK CL (Edition T)
G5R RHB

(56) Documents Cited
WO 1998/033176 A2 US 5805551 A
US 5706047 A

(58) Field of Search
UK CL (Edition S) G5R RHB RHE
INT CL[7] G11B 20/00
Online: EPODOC, WPI, PAJ.

(71) Applicant(s)
Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto, California 94304,
United States of America

(72) Inventor(s)
Keith Alexander Harrison

(74) Agent and/or Address for Service
Matthew John Lawman
Hewlett-Packard Ltd, IP Section, Filton Road,
Stoke Gifford, BRISTOL, BS34 8QZ, United Kingdom

(54) Abstract Title
Data authentication

(57) A data storage medium 10 comprising a first non-modifiable identifier 17 recorded onto it and an appended identifier 22 corresponding to the first identifier 10, the appended identifier appended to data stored on the medium 10. Access to the data is restricted based upon a comparison between the first identifier 10 and appended identifier 22. Also disclosed is a method to authenticate data stored on a medium having corresponding identifiers, a method for detecting use of counterfeited data storage media and a method to log the number of users of a piece of software.

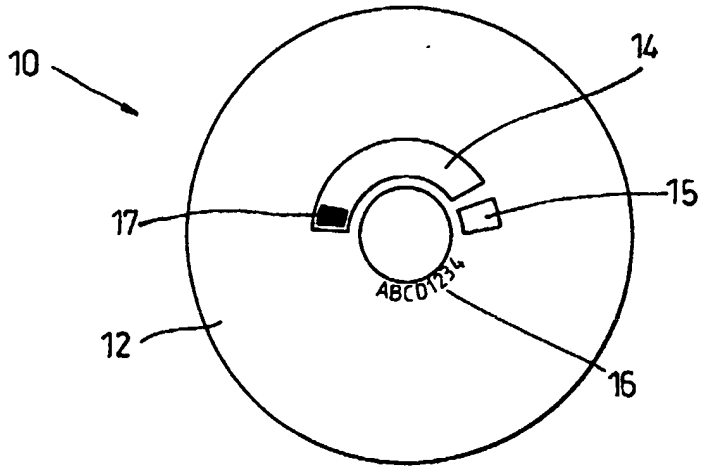

Fig. 1

GB 2 374 718 A

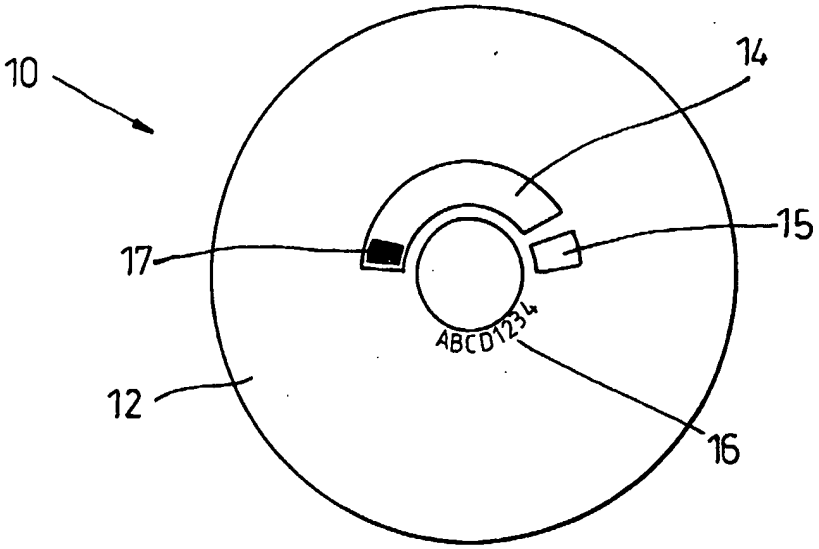

Fig. 1

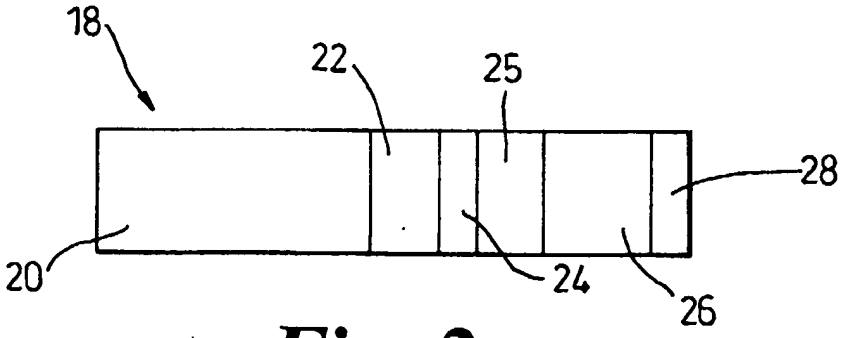

Fig. 2

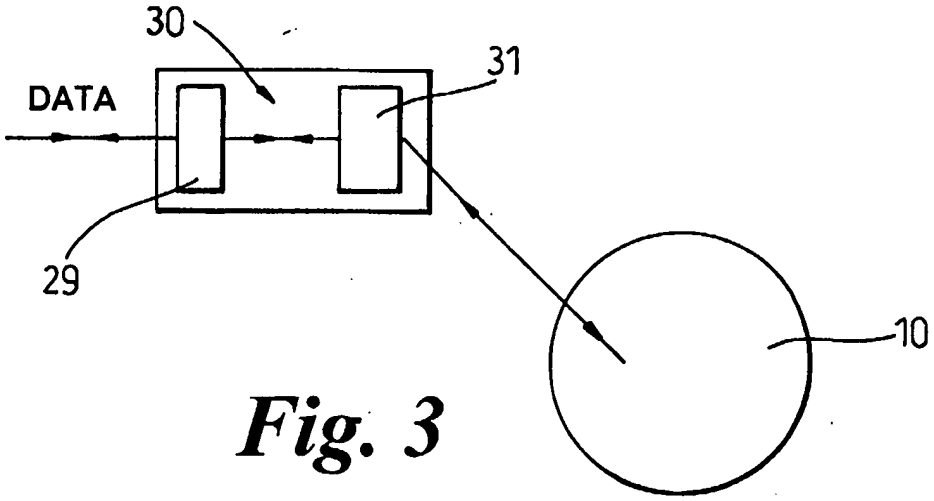

Fig. 3

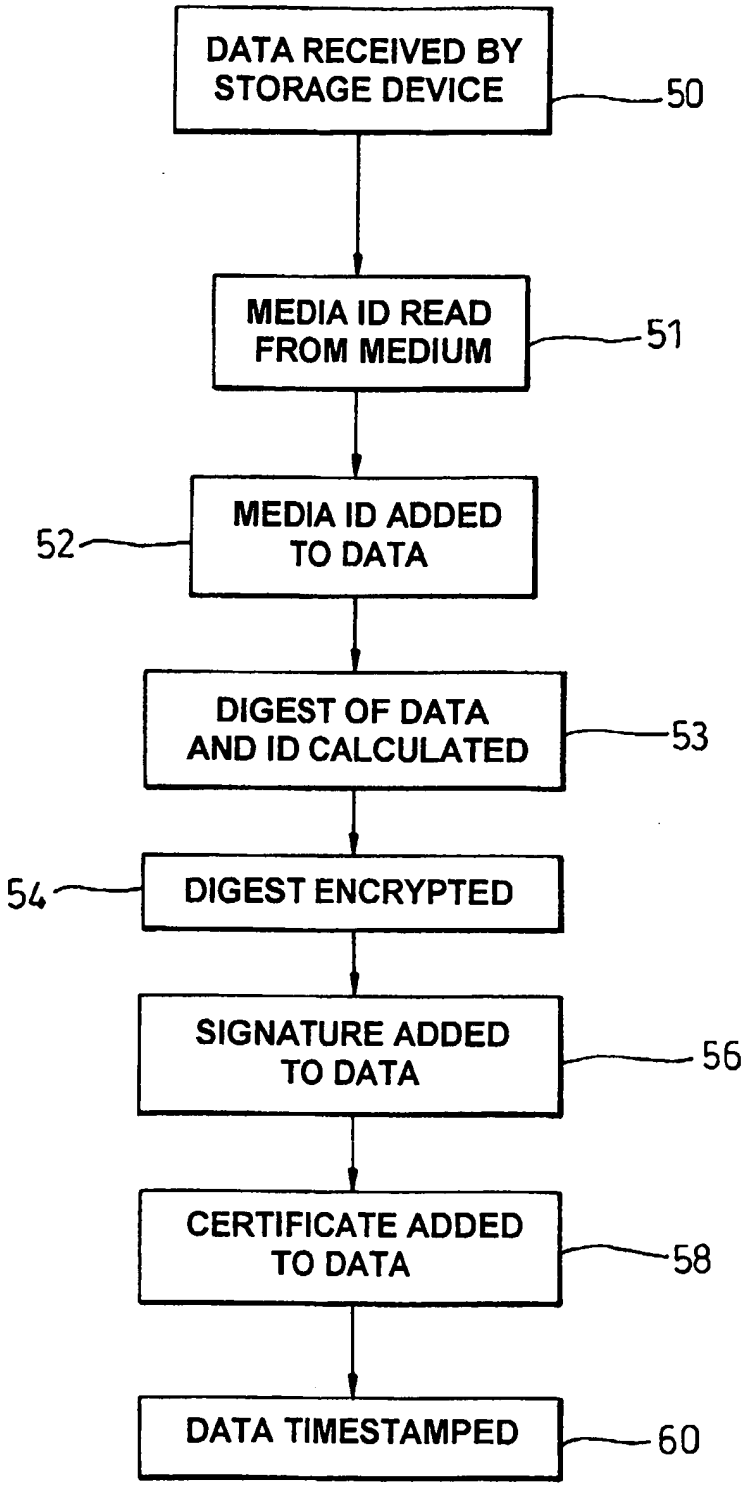
DATA RECEIVED BY STORAGE DEVICE
50
MEDIA ID READ FROM MEDIUM
51
52
MEDIA ID ADDED TO DATA
DIGEST OF DATA AND ID CALCULATED
53
54
DIGEST ENCRYPTED
SIGNATURE ADDED TO DATA
56
CERTIFICATE ADDED TO DATA
58
DATA TIMESTAMPED
60

Fig. 4

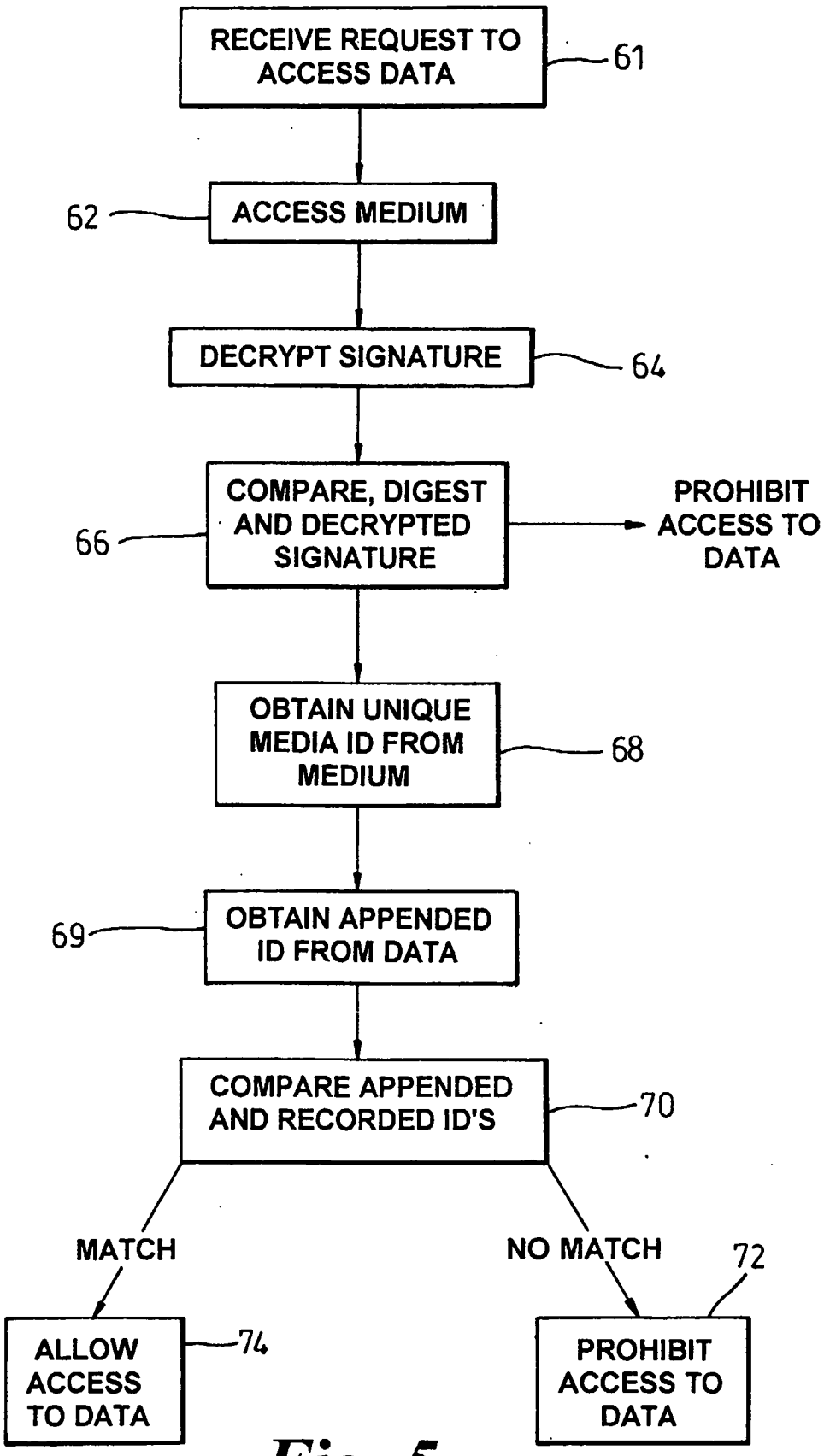
RECEIVE REQUEST TO ACCESS DATA
61
62
ACCESS MEDIUM
DECRYPT SIGNATURE
64
COMPARE, DIGEST AND DECRYPTED SIGNATURE
66
PROHIBIT ACCESS TO DATA
OBTAIN UNIQUE MEDIA ID FROM MEDIUM
68
69
OBTAIN APPENDED ID FROM DATA
COMPARE APPENDED AND RECORDED ID'S
70
MATCH
NO MATCH
72
ALLOW ACCESS TO DATA
74
PROHIBIT ACCESS TO DATA

Fig. 5

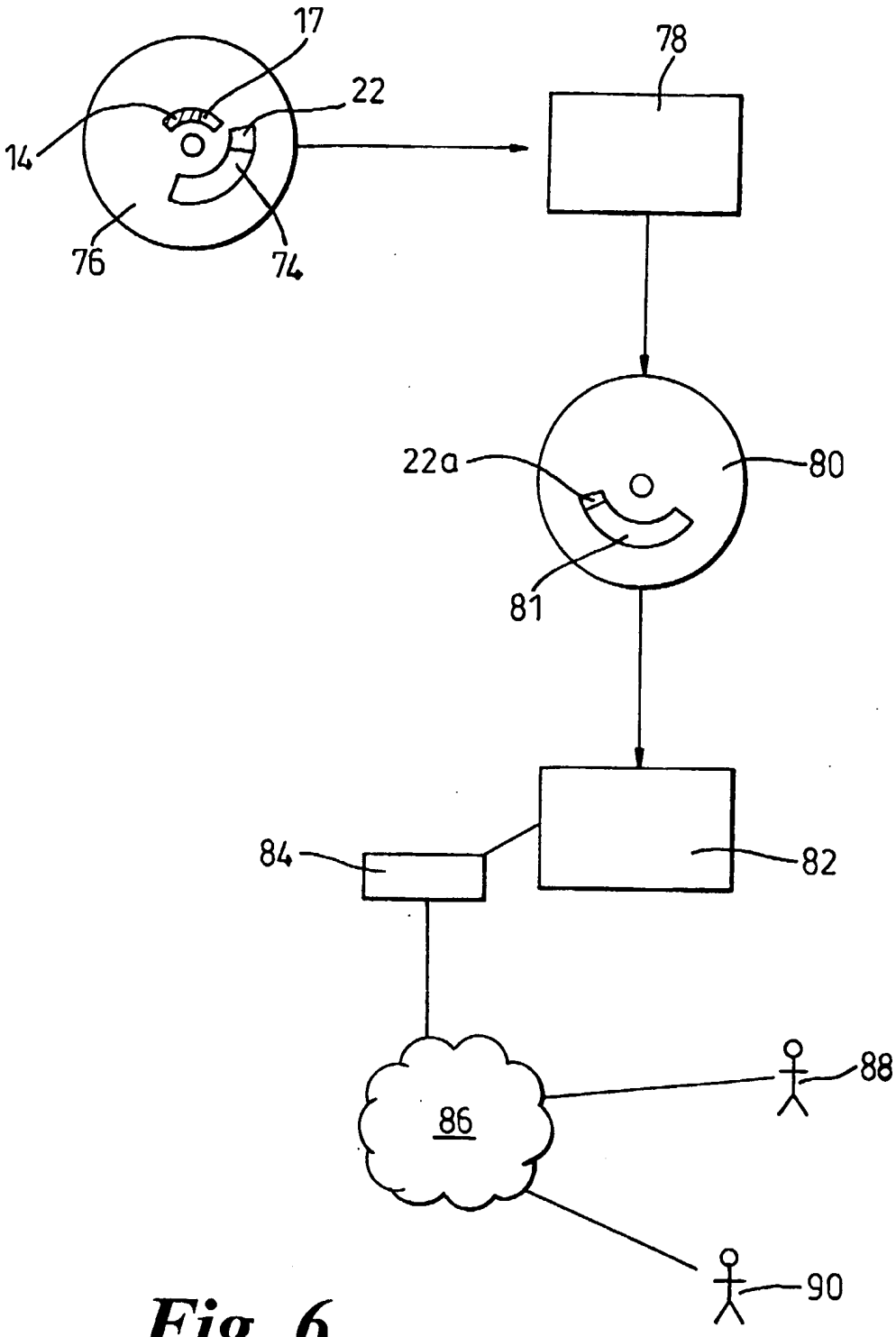

Fig. 6

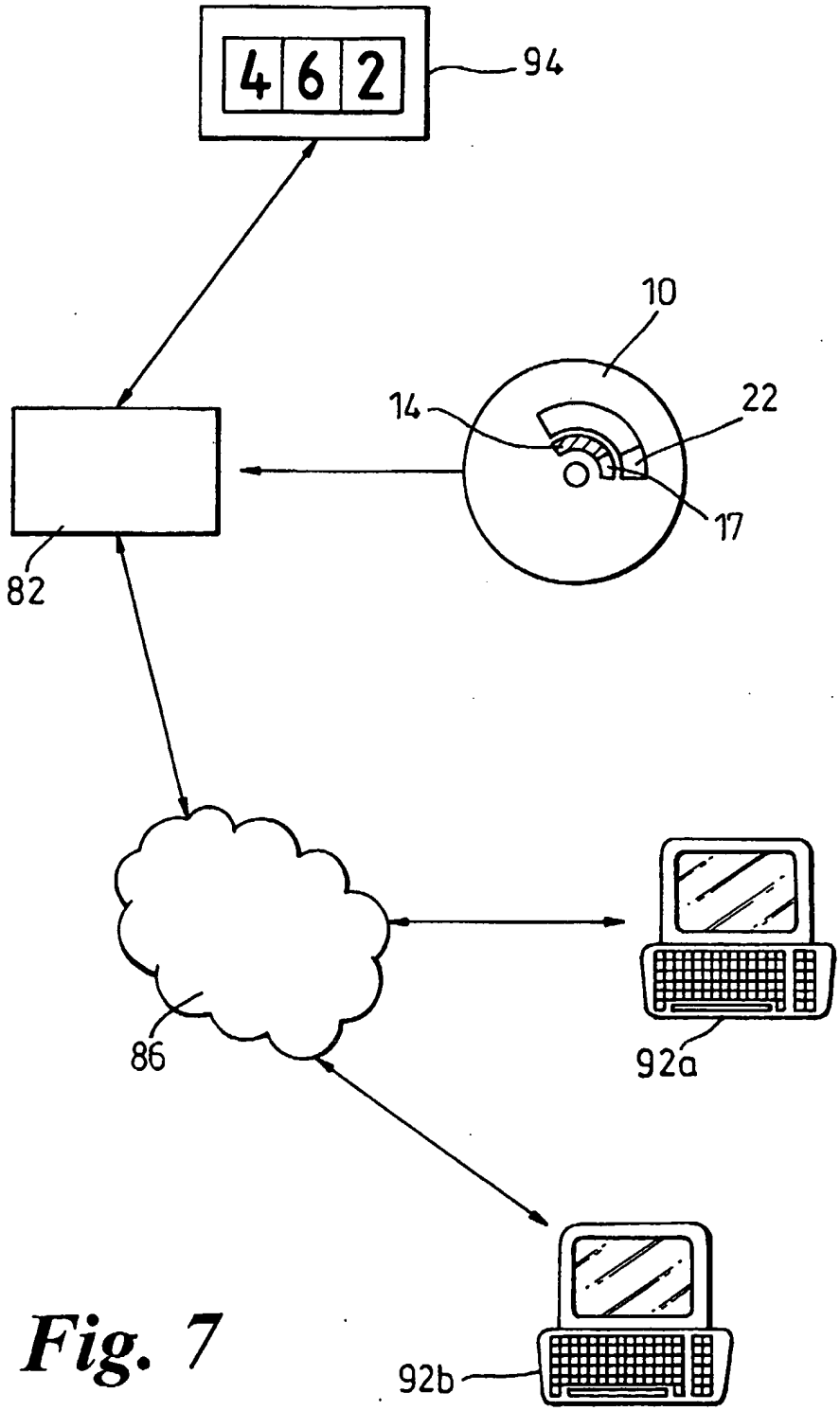

Fig. 7

DATA AUTHENTICATION

BACKGROUND OF THE INVENTION

This invention relates primarily, but not exclusively, to a method of, and data storage medium adapted for, providing authentication of a data copy. It also relates, but not exclusively, to an electronic control device, for example a PC, adapted to sample a storage medium in order to authenticate the data thereupon and/or software to adapt the electronic control device to sample the storage medium.

Currently it is very simple to obtain a perfect copy of data recorded on digital media due to the proliferation of technologies such as, for example, CD rewriters. This has led to the massive growth of counterfeiting of computer software, DVD's and music CD's. Indeed in certain areas of the world there is virtually no genuine software, it is almost exclusively counterfeit.

Manufacturers of software and entertainment products currently have no convenient way of authenticating the data stored on a medium (e.g. a CD) in such a way that the authentication can not be copied along with the data. This restricts the tracking of and quality control of products.

The ability of computers to copy data to floppy disks, the growth of MP3 players/recorders and the use of CD-rewriters to copy CD's, with no means of tracing the source data medium from which the data was copied and the machine used to copy the data, has resulted in the proliferation of untraceable copies of data.

SUMMARY OF THE INVENTION

It is an aim of, an embodiment, of the present invention to, at least partly, ameliorate, at least one of, the above-mentioned problems/difficulties.

According to a first aspect of the present invention there is provided a data storage medium having a first unique, non-modifiable, identifier associated therewith recorded thereupon.

It will be appreciated that "recorded thereupon" may mean, but is not limited to, "written onto" the medium during, or after, the manufacture process, for example a serial number printed onto a surface of the medium, "fabricated into" the medium during the manufacture process, for example a barcode or hologram formed within the medium, or it may mean a natural, physical attribute of the medium which can be used as a unique identifier.

An identifier corresponding to the first identifier may be appended to data stored on the medium, in use.

An action may be enacted based upon a comparison between the recorded identifier and the appended identifier by a device, in use. The action may be enacted if the recorded identifier and the appended identifier do not match, in use.

The action may be any one of the following non-exhaustive list: denying access to the data; restricting access to certain portions of the data; displaying a message; informing a third party.

The appended identifier may be encrypted. The encryption may be either symmetric or asymmetric. The appended identifier may form part of a digital signature. The digital signature may be certified. The appended identifier stored on the medium may be time-stamped. The timestamp may be provided by a trusted third party. The appended identifier may be the same as the first identifier or it may differ in a predetermined fashion for example an algorithm may be applied to the first identifier to scramble/encrypt to form the appended identifier. The first identifier may be a serial number. Alternatively, the first identifier may be a property of the medium, for example a refraction fringe pattern due to stress in a CD or a pattern of distributed dead sectors on a hard disk.

The first identifier (i.d.) may be a media i.d.. The first identifier may be readable by a storage device, or a PC or a processor. The storage device, PC or processors may require modification from their 'as sold' state to be able to read the first identifier. Such a modification may take the form of a plug-in card, firmware or software. The modification may be contained/concealed within the operating systems of the storage device, PC or processor. This limits the opportunities for pirates to access and decompile the modifications in order to circumvent them.

The first identifier may be non-copyable. The first identifier may be a serial number. The first identifier may be written to a non-copyable section of the medium. The non-copyable section of the medium may be made of a different material to the remainder of the medium. The first identifier may be integrally formed with the medium. The first identifier may be written to the medium at the time of manufacture of the medium. The first identifier may be stamped into a subsequently non-modifiable section of the medium. The non-modifiable section of the medium may be aluminium.

The storage device, PC or processor may read the first and the appended identifiers prior to allowing access to data stored on the medium, in use and may compare them. The storage device, PC or processor may not allow access to data stored on the medium if the first identifier is not present or has been altered, on the medium. This allows only original, first generation, copies of software to be accessed.

There may be a second identifier associated with a storage device. The second identifier may be written to the medium. The storage device may, in use, write data to the medium. The second identifier may be encrypted. The second identifier may be symmetrically or asymmetrically encrypted.

The second identifier may be a unique i.d, for example a serial number, of the storage device which, in use, wrote data to the medium. The second identifier may be written to a section of the medium which is modifiable only once, i.e. it is a 'write once-read many' section of the medium. The 'write once-read many' section of the medium may be made of a different material to the majority of the medium.

The second identifier may form part of a signature which identifies the storage device which wrote the data. The signature may also include a first identifier which identifies the medium from which the data originated. The signature may be appended to the data, in use. There may be a timestamp associated with the second identifier. The timestamp may be issued by a trusted third party. This allows manufacturers to track and find when and where a copy of a medium was made and from which original medium the copy was taken.

The second identifier may be readable by a storage device, or a PC or a processor. The storage device, PC or processors may require

modification from their 'as sold' state to be able to read the second identifier. Such a modification may take the form of a plug in card, firmware or software. The modification may be contained/concealed within the code of an operating systems of the storage device, PC or processor.

The storage device, PC or processor may read the second identifier prior to allowing access to data stored on the medium, in use. The storage device, PC or processor may not allow access to data stored on the medium if the second identifier is not present or had been altered, on the medium, or it may allow only restricted access to the data.

The storage medium may be any one of the following, non-exhaustive list; CD, CD-ROM, DVD, tape, magneto - optical disk, magnetic disk, or any form of ROM.

The storage medium may have unreadable memory elements distributed therein which form the first identifier, in use. The unusable memory elements may be randomly distributed. The magnetic disk may have unreadable second sections distributed therein which form the first identifier, in use.

According to a second aspect of the present invention there is provided a method of providing data authentication for data stored on a medium comprising the steps of:

i) assigning a first medium identifier to a data storage medium;

ii) recording the medium identifier on the storage medium;

iii) writing data to the medium from/via a data writer device;

iv) encoding the first identifier as data element; and

v) writing the encoded identifier data element to the medium in a machine readable form such that it is associated with the data.

The method may further include executing either or both of steps i) and ii) at the time of manufacture of the medium.

According to a third aspect of the present invention there is provided a method of authenticating data stored on a medium comprising the steps of:

i) searching a data storage medium for an identifier data element; and

ii) executing an action in relation to the data stored on the medium if the data element is not found or does not correspond to a media i.d. assigned to the medium.

The action may be denying access to the data stored on the medium. The action may be restricting access to certain portions of the data, for example, a virus scanning routine. The action may be creating a message for display to a user of the media. The action may be informing a third party of an attempt to access the data. The action may be to allow further copying of the data.

According to a fourth aspect of the present invention there is provided a method of data authentication comprising the second and third aspects of the present invention.

According to a fifth aspect of the present invention there is provided a data writer having a write head, the write head being adapted to write data and either, or both, of media identifiers or/and device identifiers to a storage medium according to the first aspect of the present invention.

According to a sixth aspect of the present invention there is provided a data reader having a read head, the read head being adapted to read data and either, or both, of media identifiers or/and device identifiers from a storage medium according to the first aspect of the present invention.

According to a seventh aspect of the present invention there is provided a data storage device according to the fifth and sixth aspects of the present invention.

According to an eighth aspect of the present invention there is provided a method for detecting the use of illicitly copied data storage media comprising the steps of:

i) assigning a unique identifier to a medium;

ii) recording the identifier upon a non-copyable portion of the medium;

iii) appending a data segment corresponding to the identifier to data stored upon the medium;

iv) inserting the medium into a reader and processor;

v) searching the medium for the data segment and unique identifier; and

vi a) notifying a third party if either or both of the data segment or the unique identifier are not found on the medium; or

vi b) notifying a third party if upon comparison, the data segment does not correspond to the identifier.

The method may include the step of restricting access to the data stored on the medium if either of steps vi a) or vi b) are enacted, for example by preventing virus checking. The method may further include preventing access to the data stored on the medium.

The method may further include allowing copying of the data if either of steps vi a) or vi b) are enacted.

The reader and processor may be networked. The third party may be a network manager. The third party may be an author of the data.

Steps vi a) and vi b) may involve e-mailing the notification to the third party. The e-mail may include an identifier of the reader and/or processor, for example an IP number/address.

This has the advantage of allowing network managers to know when, and possibly on which machines, illicit copies of data are being used on the networks for which they have responsibility. It may also allow authors to know if their data is being illicitly used.

According to a ninth aspect of the present invention there is provided a method of logging the number of users of a piece of software comprising:

i) providing a data storage medium according to the first aspect of the present invention;
ii) mounting the storage medium upon a reader;
iii) recording an indication that the data has been accessed; and
iv) accusing data stored upon the storage medium.

The method may further include incrementing a counter each time the data has been accessed. The method may include networking the reader.

The method may include providing the reader as a network server. The method may further include charging a user accessing the data.

This allows the use of data and/or software and/or music to be monitored and possibly charged for. In a factory environment it is possible for employees to use machinery unauthorised during scheduled downtime to produce counterfeit goods. This method allows the unauthorised use of software to be detected.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described by way of example, with reference to the accompanying drawings in which:

Figure 1 is a schematic representation of a storage medium according to one aspect of the present invention;

Figure 2 is a schematic representation of a data block to be stored on the medium of Figure 1;

Figure 3 is a schematic representation of a storage system incorporating the present invention;

Figure 4 is a flow chart showing a method of recording data according to the present invention;

Figure 5 is a flow chart showing a method of reading data according to the present invention; and

Figure 6 is a schematic representation of a copying arrangement of a medium according to the present invention; and

Figure 7 is a schematic representation of a counter arrangement according to one aspect of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

A data storage medium 10, has a major portion 12, a minor portion 14 and a write once-read many portion 15. The major portion 12 is typically read-write; thereby allowing reuse of the data storage medium 10.

The minor portion 14 is typically read-only thereby preventing the alteration of any data which is recorded thereupon. A unique media identifier (i.d.) 17 which identifies the medium 10 is encoded and stored as an identification block 16 within the minor portion 14.

A data block 18 intended, to be written, to the medium 10 comprises body data 20, a data segment 22 which corresponds to the unique media i.d. 17 and a digest 24. The digest 24 is a digest of the body data 20 and the data segment 22 and may be encrypted to form a signature 25.

Digital signatures reduce the opportunities for data tampering and falsification. This involves passing the data through a hashing algorithm to obtain a digest of the message. The digest is then encrypted using an asymmetric encryption private key to provide a signature. The signature is appended to the data and transmitted with it.

A third party who has the public key which is complementary to the private key used in the encryption process can decrypt the signature to obtain the digest. The third party can rehash the received data and calculate the digest of this. The digest from the signatures and the

rehashed digest are compared, if they do not match then the data has been tampered with.

The data block 18 may, optionally include a certificate 26 issued to the author of the data 20 and a timestamp 28. The certificate 26 can include the public key necessary to decrypt the signature 25.

Certificates are electronic documents which attest to the identity of the person from whom the document came. They are issued by trusted identity certification authorities and have an expiry date to reduce the time available for them to be hacked or cracked.

The timestamp 28 serves to verify that the data block 18 was signed prior to the expiry of the certificate 26 and can be provided by a trusted third party.

WRITING DATA TO THE DATA CARRIER

The body data 18 is received from a data source by an interface 29 of a storage device 30. (step 50). The unique media i.d. 17 is read from the medium (step 51) and added to or associated with the body data 18 (step 52) as an i.d. data segment 22, typically either a header or a footer. This "body data and media ID" information is temporarily held in the device 30.

The combined digest 24 of the data 18 and the data segment 22 is calculated (step 53) by the device 30, for example by using a hash function. The digest 24 is encrypted (step 54) using a private key owned by the author of the data to form the signature 25 (step 56). This is appended to the body data 20, and data segment 22.

In some embodiments a certificate containing a public key corresponding to the private key, can be appended (step 58) to the data block 18. This identifies the author of the data and has an expiry date. The temporal limit on the validity of a certificate 26 resists the opportunities for the cracking/hacking of the private key associated with the certificate. A trusted third party may timestamp the data (step 60) in order to verify that the data was recorded prior to the expiry of the certificate 26.

READING DATA FROM THE DATA CARRIER

Upon receiving a request to access the body data 20 (step 61) a processor 31 associated with a storage device 30 accesses the medium 10 (step 62) and decrypts (step 64) and compares the signature 25 to a calculated hash of the body data and unique i.d. using the public key in the normal way (step 66) This ensures that the data, and the appended data segment 22 have not been tampered with or altered.

The processor 31 again accesses the medium 10 in order to obtain the unique media i.d. 17 from the minor portion 14 of the medium 10 (step 68) and the appended i.d. is obtained from the data segment 22 (step 69). The i.d. 17 obtained from the minor portion 14 is compared to that obtained from the data segment 22 (step 70).

If the two media i.d. 17, 22 do not correspond to each other this is taken as an indication that the data 18 has been illicitly copied from another, source media. The processor 31 can be adapted to refuse to access (step 72) data for which the medium 10 media i.d. 17 does not match that in the data segment 22 or for which the signature 25 gives evidence of tampering with the data/recorded i.d. The processor 31 can allow access to the data if the media i.d. 17 matches that in the data segment 22 (step 74).

Either or both of the processor 31 or storage device 30 may require adaptation in order to allow it to access of the media i.d. 17 stored in the minor portion 14 of the medium 10 and compare this to the data segment 22 appended to the body data 18. This can be achieved in a number of ways for example, software alterations to the operating system, firmware or hardware additions to the systems of either or both of the processor 31 or storage device 30.

It is envisaged that each data storage device 30 could have its own unique i.d. which is written to the write once-read many portion 15 of the medium 10, for example, at the same time as the writing of the data block 18 to the medium 10. The storage device 30 i.d. can be incorporated into the signature 25. Thus, it is possible to track the reproduction of the data with reference to the storage device 30 upon which the copy was made.

In use, a first CD 76 bearing a unique media i.d. 17 is inserted in a CD rewriter 78 a copy of data stored on the first CD 76 is made to a second CD 80. The copy of the data include a copy of the unique media i.d. 17 which was appended to the data as a data segment 22. However, as the hard-written unique media i.d. 17 is recorded upon a non-copyable portion 14 of the first CD 76 it is not possible to transfer this to the second CD 80.

When the second CD 80 is inserted in a reader 82, for example on a PC, DVD player, music system or network server, which is in accordance with an aspect of the present invention, the reader 82 can decrypt the data segment 22 containing the copy of the unique media i.d.17 but will not be able to locate the hard-written copy of unique media i.d. 17 on the second CD 80. The reader will attempt to compare the decrypted data segment media i.d. 22 with the hard-written media i.d. 17.

Upon failing to read the hard-written media i.d. 17 the reader 82 can deny access to the data contained upon the second CD 80. Alternatively the reader 82 may restrict access to certain portions of the data, for example a virus scanning routine as if a copy has been made the author of the data makes no guarantees and accepts no liability for any viruses present upon the media 10. As a second alternative the reader 82, in conjunction with a processor 84 may produce a message, either audio or visual, which informs a potential user of the illicit copy that for example, they are using an illegal copy and should desist. As a third alternative, if the reader 82 and a processor 84 are connected to a network 86, for example the Internet, it is possible to send a message over the network 86 informing either, for example, a network manager 88 or the author 90 of the software that an illicit counterfeit copy is attempted to be loaded on the network 86. This may reduce office liability for counterfeit software use, as it would allow the network manager to act swiftly to eradicate such abuses.

It will be appreciated that references to datain the preceding paragraphs relate to any form of data e.g. text, video, audio (for example sound, music, recordings), computer programs, databases or the machine readable codes.

It will further be appreciated that although reference has been made to first and second CD's either of the first and second media could be any one of tape, magnetic-optical disks, DVD, magnetic disk, or ROM.

The reader 82 can act as a network server and data on a medium 10 mounted thereupon can be accessed via the network 86 by a plurality of devices 92a, 92b, shown in Figure 7, as PC's. The devices could be any one of a PC, storage device, DVD, music player or server. Each time the

medium 10 is accessed an indentifier of the devices, for example 92a, accessing the medium 10 is recorded and a counter 94 is incremented. The counter 94 can be internal of the reader 82 or can be a separate external device such as a PC or server. A counter can be arranged for each device 92a, 92b or a single counter can count the total number of times the medium is accessed.

This arrangement allows users accessing the data on the medium 10 to be charged for the number of times they access the data. Each user may have an identifier such as a PIN which increments their individual counter whichever device 92a, 92b they access the data from.

CLAIMS

1. A data storage medium (10) comprises a first unique, non-modifiable identifier (17) associated therewith recorded thereupon.

2. A medium as claimed in claim 1, wherein an identifier (22) corresponding to the identifier (17) is appended to data stored on the medium (10), in use.

3. A medium as claimed in either of claims 1 or 2 wherein an action is enacted based upon a comparison between the first identifier (17) and the appended identifier (22) by a device (30), in use.

4. A medium as claimed in claim 3 wherein the action is enacted if the first identifier (17) and the appended identifier (22) do not match, in use.

5. A medium as claimed in either of claims 3 or 4 wherein, in use, the action is any one, or combination of the following: denying access to the data; restricting access to certain portions of the data; displaying a message; informing a third party.

6. A medium as claimed in any one of claims 3 to 5 wherein the device (30) which accesses the data stored on the medium is any one or combination of a storage device, PC or a processor.

7. A medium as claimed in any one of claims 3 to 6 wherein there is a second identifier associated with the device (30).

8. A medium as claimed in any one of claims 3 to 7 wherein there is an identifier associated with the device (30) which is written to the medium (10) when data is written thereto, in use.

9. A medium as claimed in any one of claims 2 to 8 wherein the appended identifier (22) and the first identifier (17) differ in a predetermined fashion.

10. A medium as claimed in any one of claims 2 to 9 wherein the appended identifier (22) and the first identifier (17) are identical.

11. A medium as claimed in any one of claims 2 to 10 wherein the appended identifier (22) is encrypted, in use.

12. A medium as claimed in any one of claims 2 to 11 wherein the appended identifier (22) forms part of a digital signature (25), in use.

13. A medium as claimed in any preceding claim wherein the first identifier (17) is non-copyable.

14. A medium as claimed in any preceding claim wherein the first identifier (17), in use, is written to a non-copyable section (14) of the medium (10).

15. A medium according to any preceding claim wherein the first identifier (17) has a time-stamp (28).

16. A method of providing data authentication for data stored on a medium comprising the steps of:

i) assigning a first medium identifier (17) to a data storage medium (10);

ii) recording the medium identifier (17) on the storage medium (10);

iii) writing data to the medium (10) from/via a data writer device (78);

iv) encoding the first identifier (17) as data element (22); and

v) writing the encoded identifier data element (22) to the medium (10) in a machine readable form such that it is associated with the data.

17. A method of authenticating data stored on a medium comprising the steps of:

i) searching a data storage medium (10) for an identifier data element (22); and

ii) executing an action in relation to the data stored on the medium (10) if the data element (22) is not found or does not correspond to a media identifier (17) assigned to the medium (10).

18. A method as claimed in claim 17 wherein the action is denying access to the data stored on the medium (10).

19. A method as claimed in claim 17 wherein the action is restricting access to data stored on the medium (10).

20. A method as claimed in one of claims 17 to 19 wherein the action includes creating a message for display to a user of the medium (10).

21. A method as claimed in any one of claims 17 to 21 wherein the action includes informing a third party (88, 90) of an attempt to access the data.

22. A method as claimed in claim 17 wherein the action is to allow copying of the data.

23. A method of data authentication comprising a combination of any one of claims 16 and 22.

24. A data writer having a write head, the write head being adapted to write data and either, or both, of media identifiers or/and device identifiers to a storage medium according to any one of claims 1 to 15.

25. A data reader (82) having a read head, the read head being adapted to read data and either, or both, of the media identifier or/and device identifier from a storage medium according to any one of claims 1 to 15.

26. A data storage device being a combination of the data writer of claims 24 and the data reader (82) of claim 25.

27. A method for detecting the use of illicitly copied data storage media comprising the steps of:

i) inserting a medium into a reader (82) or processor (84);

ii) searching the medium for a data segment and a unique identifier; and

iii a) notifying a third party if either or both of the data segment or the unique identifier are not found on the medium; or

iii b) notifying a third party if upon comparison, the data segment does not correspond to the identifier.

28. A method as claimed in claim 27 including the step of restricting access to data stored on the medium (10) if either of steps iii a) or iii b) are enacted.

29. A method as claimed in claim 27 including the step of denying access to data stored on the medium (10) if either of the steps iii a) or iii b) are enacted.

30. A method as claimed in claim 27 including the step of allowing copying of the data stored on the medium (10) if either of the steps iii a) or iii b) are enacted.

31. A method as claimed in any one of claim 27 to 30 including the step of connecting the reader (82) and the processor (84) to a network (86).

32. A method as claimed in claim 31 wherein the third party is a network manager (88).

33. A method as claimed to 31 wherein the third party is the author (90) of the data.

34. A method as claimed in any one of claims 31 to 33 wherein steps iiia) and iii b) include e-mailing the notification to the third party (88, 90).

35. A method as claimed in claim 34 wherein the e-mail includes the an identifier of either or both of the reader (82) or/and processor (84).

36. A method of logging the number of users of a piece of software comprising:

i) providing a data storage medium (10) according to any one of claims 1 to 12;

ii) mounting the storage medium (10) upon a reader (82);

iii) recording an indication that the data has been accessed; and

iv) accessing data stored upon the storage medium (10).

37. A method as claimed in claim 36 including the step of networking the reader (82).

38. A method as claimed in claim 37 including the step of providing the reader as a network server (82).

39. A method as claimed in any one of claims 36 to 38 including the step of incrementing a counter (94) each time the data is accessed.

40. A method as claimed in any one of claims 36 to 39 including the step of charging a user accessing the data.

INVESTOR IN PEOPLE

Application No:	GB 0109034.9	**Examiner:**	Eleanor Thurston
Claims searched:	1-35	**Date of search:**	30 October 2001

22

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G5R (RHB, RHE)

Int Cl (Ed.7): G11B 20/00.

Other: Online: EPODOC, WPI, PAJ.

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	WO 98/33176 A2	(KONINKLIJKE PHILIPS) see abstract.	1-4, 9, 13 at least.
X	US 5805551 A	(OSHIMA et al) see abstract and column 2. lines 46-65.	1-5 at least.
X	US 5706047 A	(LENTZ et al) see abstract, figure 5.	1, 2 & 13 at least.

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.